شماره شش

قبیله گیک ها

امنیت (دو)

تنها مجله مخصوص گیک های ایرانی

فهرست

سخن سردبیر

اگر به متن قوانین حمورابی توجه کنید متوجه خواهید شد که قوانین او نیز در طول زمان و بر اساس شرایط و تجربیات انسانها دستخوش تغییر و دگرگونیهای بسیاری شده است. به نظر ما این موضوع نشان دهنده آن است که حتی مطالبی که در دل سنگ حک شده اند نیز نمیتوانند جاودانه و بی نقص باشند، در طول زمان و با افزایش علم و دانش، انسانها ناچار به تغییر میباشند و یا اینکه مانند همان نوشته های کنده کاری شده بر سنگ در حد یک جاذبه تاریخی باقی خواهند ماند. منظور از بیان این موضوع مقدمه سازی برای اعلام فصل جدیدی در (قبیبله گیک ها) است. بعد از انتشار پنج شماره و آزمون و خطاهای بسیار در این مدت و با استفاده از پیشنهادات و انتقادات سازنده شما همراهان همیشگی مجله و برای اینکه به جاذبه ای تاریخی تبدیل نشویم تغییرات بنیادی را در روش تولید محتوا و نحوه انتشار آنها ایجاد کردیم تا بتوانیم مطالب مفیدتری را با روشی بهتر در اختیار شما قرار دهیم. از این پس سعی خواهیم کرد تا مطالب دنباله دار در چند شماره ارائه دهیم. همچنین آموزشهایی هر چند کوتاه در زمینه های تخصصی ارائه خواهیم داد. درکنار این موارد سعی میکنیم که هر موضوع (تم) مجله را حداقل در ۳ شماره پیاپی دنبال نمائیم تا بتوانیم مطالب را بهتر و کاملتر در اختیار شما خوانندگان عزیز قرار دهیم. از زمانی که مجله قبیله گیک ها اعلام وجود کرد تیم نویسدگان این مجله همیشه در حال تغییر بوده است ولی بعد از گذشت ۶ ماه باالاخره تیم اصلی نویسندگان قبیله گیک ها مشخص شد و ۱۰ نفر گیک متعهد در کنار یکدیگر جمع شدند تا در هر ماه با نوشتن مطلبی در حد یک یا دو صفحه موضوعی جدید را به دیگر دوستان خود یادآوری کنند

در این مدت گیک های متفاوتی چه در قالب مصاحبه شوندگان و چه در قالب منتقدان و یا موارد دیگر به ما کمک های فراوانی کردند و ما آنها را نیز عضوی از قبیله گیک ها میدانیم.

بسیاری از ما میپرسند که چرا "قبیله گیک ها" وب سایت رسمی ندارد؟ باید برای این دوستان توضیح دهیم که ما در قبیله گیک ها خود را بصورت گیک های چادر نشین دنیای اینترنت میبینیم که در سطح اینترنت و بر روی پلتفورم های متفاوت زندگی میکنیم و هر از چندی بصورت قبیله ای در یک پلتفورم به دور هم جمع میشویم. در حال حاضر تلگرام را محلی برای برپائی چادرهای قبیله خود انتخاب نموده ایم و همگی به دور هم در تلگرام با هم در ارتباط هستیم و تا زمانی که بر روی تلگرام خوش بگذرد بر روی آن خواهیم بود و کانال رسمی ما بر روی تلگرام فعالیت میکند. اگر در آینده به پیام رسان دیگری نقل مکان کردیم کانال رسمی خود را بر روی آن برپا خواهیم نمود.

برای ما دوستی که بین اعضای قبیله بوجود آمده است اهمیت دارد نه برپا کردن سایت برای قبیله. بنای قبیله ما بصورتی برپا شده است که میتوانیم با یکدیگر در هر جای اینترنت در ارتباط باشیم بدون وابستگی به محل یا سیستم خاصی.

ما معتقدیم داشتن سایت ما را یکجا نشین میکند و ما مایل هستیم بر روی اینترنت با آزادی تمام چادر برپا کنیم.

در آخر باز هم لینک گروه چت تلگرام قبیله گیک ها را برای اطلاع شما قرار میدهیم.

https://telegram.me/joinchat/BMcoYj4zho8sEcN-QP_iUg

موفق باشید.

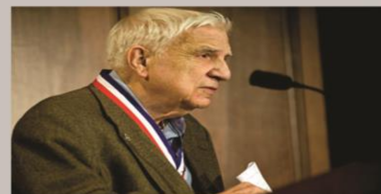
@BOBZBOBZ

تقویم تاریخ

راجر ایستون متولد ۳۰ آوریل ۱۹۲۱

ایشون در کالج به تحصیل در رشته فیزیک پرداخت، در سال ۱۹۵۵ یکی از کسانی بود که طرح مهمی رو به نام سامانه موقعیت یاب جهانی به وزارت دفاع آمریکا ارائه کرد. این طرح یکی از ایده‌هایی بود که راجر اونرو پرورش داده بود، اما طرح راجر مورد تایید وزارت دفاع آمریکا قرار نگرفت. ایشون به کارش ادامه داد تا اینکه تاییدیه پیاده سازی سیستم در حالت آزمایشی رو دریافت کرد و در ابتدا با ۴ ماهواره شروع به پیاده سازی سیستم موقعیت یاب جهانی کرد. آزمایش راجر ایستون در سال ۱۹۷۷ با موفقیت انجام شد و ماهواره NTS-۲ اولین سیگنال‌های GPS رو به زمین ارسال کرد. طرح اولیه GPS با اهداف نظامی بود اما از سال ۱۹۸۰ میلادی این سیستم با اهداف غیر نظامی هم مورد استفاده قرار گرفت.

سامانه موقعیت یاب جهانی یا Global Positioning System سامانه منظومه‌ای تشکیل شده از ۲۴ ماهواره است که به دور زمین در حال گردش هستن و در هر مدار ۴ ماهواره قرار داره. این ماهواره‌ها از محاسبات ریاضی ساده‌ای برای پخش اطلاعات استفاده می‌کنن که به عنوان طول و عرض و ارتفاع جغرافیایی، به وسیله ی گیرنده های زمین دریافت می‌شن. جی پی اس در تمام شرایط به صورت ۲۴ ساعت در شبانه روز و در تمام دنیا قابل استفاده است و همونطور که میدونید هیچ هزینه ای بابت این خدمات دریافت نمیشه. ماهواره‌های جی پی اس، هر روز دو بار در یک مدار دقیق دور زمین میچرخن و سیگنال‌های حاوی اطلاعاتو به زمین می فرستن.



مریم میرزاخانی متولد ۱۳ اردیبهشت ۱۳۵۶، تهران، ریاضی‌دان و استاد ایرانی دانشگاه استنفوردِ آمریکا.

ایشون اولین دختریه که به تیم المپیاد ریاضی ایران راه پیدا کرده، تو المپیاد ریاضی ایران طلا گرفته و اولین کسیه که تو آزمون المپیاد ریاضی جهانی نمره کامل گرفت. مدرک کارشناسیشونو در رشته ریاضی از دانشگاه شریف گرفتن و سال ۱۹۹۹ برای ادامه تحصیل دکترا به دانشگاه هاروارد رفتن. ایشون همچنین اولین بانوی ریاضیدان تاریخ لقب گرفت که تونسته مدال فیلدز، معتبرترین جایزه دنیای ریاضیات رو به دلیل تلاش هاش در زمینه هندسه پیشرفته و جا به جایی های فضایی به خودش تخصیص بده. مدال فیلدز، بالاترین نشان علمی رشته ریاضیاته که هر چهار سال یک بار به دانشمندان برگزیده زیرِ ۴۰ سالِ جهان اهدا می‌شه.



سال ۱۹۹۹ میلادی ایشون موفق شد راه حلی برای یه مشکل ریاضی پیدا کنه. خیلی از ریاضیدان ها برای مدت زمان زیادی دنبال پیدا کردن روشی برای محاسبه حجم رمزهای جایگزین فرم‌های هندسی هذلولی بودن و اینجا بود که خانم میرزاخانی جوان تو دانشگاه پرینستون نشون داد که با استفاده از ریاضیات، شاید امکانش باشه که بهترین روش رو برای پیدا کردن راه حلی روشن در اختیار داشته باشیم. میرزاخانی همچنین به فکر اینه که معمای ابعاد گوناگون فرم‌های غیر طبیعی هندسی رو حل کنه. البته اگر جهان از قاعده هندسه هذلولی تبعیت کنه، این ابتکار به تعریف شکل و حجم دقیق جهان کمک میکنه.

پیر ویکتور اوگر، ۱۴ می ۱۸۹۹

پیر تحصیلات مقدماتی و دبیرستان را در پاریس "گذروندن و سپس وارد دانشگاه اِکول نرمال سوپریور در فرانسه شد و تا سال ۱۹۲۲ همونجا به تحصیل پرداخت. بعد از فارغ التحصیلی وارد لابراتوار شیمی فیزیک دانشگاه پاریس شد و زیر نظر ژان پرین، فیزیکدان بزرگ فرانسوی به تحقیق درمورد پدیده فوتوالکتریک پرداخت و تحصیلاتشو هم ادامه داد.



در سال ۱۹۲۶ ایشون موفق شد دکترای فیزیکشو از دانشگاه پاریس دریافت کنه. بعد از فارغ التحصیلی، بیشتر زمانشو به تدریس و تحقیق در دانشگاه های مختلف فرانسه پرداخت، که البته این فعالیت‌ها در خلال جنگ جهانی دوم و اشغال فرانسه با کمی وقفه مواجه شد. دکتر اوگر تغییرات زیادی در سطح تحصیلات تکمیلی سیستم آموزشی فرانسه ایجاد کرد که برای نمونه میشه به راه‌اندازی رشته ژنتیک در دانشگاه سوربون اشاره کرد. مهم‌ترین دستاورد اوگر به تحقیقاتش راجع به پرتوهای کیهانی برمیگرده. پرتوهای کیهانی ذراتی هستن که در فضای خارج از اجرام آسمانی تولید شدن و به جو این اجرام برخورد می‌کنن. این کشف دکتر اوگر کمک زیادی به شناخت علت شکل‌گیری پدیده رگبار آسمانی کرد و نشون داد چرا این پدیده لزوما تو هر شرایطی شکل نمی‌گیره، همچنین ثابت کرد که بخشی از انرژی پرتوهای کیهانی در زمان برخورد با جو زمین کاهش پیدا می‌کنه.

@Sh_Ebrahiimii

CompTIA Security+ چیست؟

مدارک CompTIA به خوبی در مجامع IT و بخصوص به عنوان اعتباری برای استخدام شوندگان IT توانسته اند خود را مطرح کند. مایکروسافت، سیسکو، Novell و دیگر شرکت های صاحب سبک در زمینه IT این اجازه را دادند تا از مدارک CompTIA در برخی از برنامه هایشان به عنوان انتخاب و یا جایگزینی برای یکی از امتحانات استفاده شود. برای مثال مدارک CompTIA A+ و Network+ میتوانند در ادامه مدرک MCSA مایکروسافت، اخذ شوند. یکی از مزیت های امتحانات و مدارک CompTIA که آن ها را بسیار محبوب کرده است، این است که بر خلاف سایر مدارک موجود در این زمینه از موسسات مختلف، این مدارک بازه زمانی ندارند. در حقیقت وقتی که شما مدرک CompTIA را اخذ میکنید، هرگز نیازی به تمدید آن ندارید.

مسیری که برای گرفتن مدرک Security+ باید طی شود:

فقط یک امتحان برای اخذ این مدرک کافی است. اما باید دقت داشت که این امتحان بسیار سنگین بوده و محدوده وسیعی از مفاهیم امنیتی شامل موارد زیر را در بر میگیرد:

مفاهیم عمومی امنیت

امنیت ارتباطات

امنیت زیرساخت

پایه های رمزنگاری

امنیت سازمانی/ اجرایی

پیش نیازها و آماده سازی:

در مقایسه با مدارک دیگر امنیت مثل CISSP و SANS GIAC، مدرک+security یک مدرک پایه برای ورود به دنیای امنیت محسوب میشود و هیچ پیش نیازی (آزمون ها یا مدارک قبلی) برای شرکت در این آموزن وجود ندارد. هرچند این نکته را نیز باید اضافه کرد که شرکت CompTIA شرط حداقل دو سال سابقه کار مفید در زمینه IT را برای اخذ مدرک الزامی کرده است.

این پیش شرط به این جهت قید شده است تا از اعتبار مدارک CompTIA کاسته نشود. گذراندن دوره های +A و +Network پیش از CompTIA Securi-+ ty، اگرچه الزامی نیست ولی باعث میشود تا پایه و زمینه خوبی جهت درک بهتر مباحث امنیتی حاصل شود و این موضوع از طرف خود CompTIA هم توصیه شده است. تجربه های کم ولی پایه ای و ارزشمند ما از کار با دیوایس ها و نرم افزارهای امنیتی، مانند فایروال ها، سرویس های Certificate، شبکه های خصوصی مجازی (VPN)، دسترسی وایرلس و نظایر آن در این دوره ضمن آن که مورد پوشش قرار میگیرد و کامل میشود، بطور جدی نیز محک زده خواهد شد؛ اگرچه که میتوان گفت بدون این تجربه ها هم میشود از پس این دوره برآمد.

معرفی مفاهیم عمومی امنیت:

این بخش به معرفی سه گانه AAA از مفاهیم امنیتی میپردازد:



کنترل دسترسی (access control)، احراز هویت (au-thentication) و بازرسی (auditing). دانشجویان این دوره همچنین با اصطلاحات موجود در زمینه امنیت کامپیوتر آشنا خواهند شد و درباره اهداف اصلی امنیت شبکه/کامپیوتر یعنی ایجاد محرمانگی داده، حفظ یکپارچگی دیتا و اطمینان در دسترس بودن اطلاعات برای کاربران مجاز یاد آموزش میبینند.

کنترل دسترسی:

این بخش بر راه هایی که متخصصان امنیت شبکه میتوانند دسترسی موجود بر منابع شبکه را در کنترل خود داشته باشند تمرکز دارد و درباره سه نوع مهم از کنترل های دسترسی یعنی دسترسی کنترل اجباری (MAC)، دسترسی کنترل بر اساس مصلحت (DAC) و دسترسی کنترل مبتنی بر وظیفه (RBAC) به صحبت میپردازد.

احراز هویت:

این بخش بسیاری از روش های موجود در احراز هویت کاربران و کامپیوترها را در یک شبکه پوشش میدهد. در تمامی این روش ها هویت یک کاربر و یا یک کامپیوتر قبل از برقراری یک session ارتباطی، اعتبار سنجی میشود. در ادامه پروتکل های استاندارد صنعتی بررسی خواهند شد که شامل Ker-beros (در هر دو پلت فرم یونیکس و سیستم عامل های جدید ویندوز برای احراز هویت درخواست های کاربران جهت دسترسی به منابع) و پروتکل CHAP که در احراز هویت کاربران ریموت استفاده میشود، هستند.

پس از آن درباره استفاده از گواهی های دیجیتال، توکن ها و احراز هویت یوزر/پسورد بحث خواهد شد. احراز هویت های چند پارامتری (که در احراز هویت های چندگانه جهت امنیت بیشتر استفاده میشود)، احراز هویت متقابل (احراز هویت دو طرفه بین کلاینت و سرور) و احراز هویت بیومتریک (از خصوصیات فیزیکی شما برای شناسایی هویت استفاده میکند)، همگی مورد بررسی قرار خواهند گرفت.

سرویس ها و پروتکل های غیرضروری:

این بخش درباره آن دسته از سرویس ها و پروتکل هایی بحث میکند که غالبا بصورت پیش فرض بر روی سیستم های شبکه نصب میشوند که دربسیاری از موارد، زمانی که نیازی به اجرای آن ها نیست، جهت برقراری امنیت بیشتر میتوان آن ها را غیرفعال نمود.

حملات:

این بخش برخی از اکسپلویت های مرسوم که توسط هکرها برای حمله و یا اختلال در سیستم ها استفاده میشود را توضیح میدهد. به عنوان نمونه ای از این موارد میتوان به حملات منع سرویس (DoS) حملات بکدور، spoofing، حملات TCP/IP hijacking، reply، MITM، کلیدهای ضعیف و اکسپلویت های محاسباتی، روش های کرک پسورد و اکسپلویت های نرم افزار اشاره نمود.

CompTIA Security+

در تمامی این مراحل جزئیات فنی درباره نحوه کارکرد این حملات داده نمیشود، اما درباره نحوه جلوگیری، شناسایی و پاسخ دهی به این حملات مطالبی را آموزش خواهید دید.

هندسی اجتماعی

در این بخش به بررسی پدیده استفاده از مهارت های اجتماعی (نقش بازی کردن، جذاب بودن، توانایی متقاعد کردن) در بدست آوردن اطلاعاتی (مثل پسوردها و نام اکانت ها) که برای ورود غیرمجاز به یک سیستم و یا شبکه لازم است، پرداخت میشود.

کدهای مخرب

در این بخش به بررسی ویروس های کامپیوتری، برنامه های تروجان، بمب های منطقی، worm ها و دیگر بدافزارهای مخرب که غالبا از طریق شبکه به سیستم - سهوا و یا عمدا- وارد میشوند، پرداخته میشود.

بازرسی و پیگیری لاگ ها

در این بخش به روش هایی که متخصصان امنیت میتوانند از لاگ ها و ابزارهای اسکن سیستم برای جمع آوری اطلاعات (اطلاعاتی که به حملات و ایجاد اختلال کمک میکنند)استفاده کنند، گذری خواهد داشت. با این روش میتوان قبل از اینکه اتکرها باگ های امنیتی موجود در شبکه و یا سیستم را پیدا کنند، آن ها را شناسایی و نسبت به برطرف سازی آن ها اقدام کرد.





@rooham_inet

تفاوت گیک و نرد در نرم افزار

برای اینکه بتوانیم تفاوت بین گیک و نرد را در نرم افزار بهتر درک کنیم باید در مرحله اول تعریفی از این دو داشته باشیم. ابتدا تعریفی از گیک خواهیم داشت. اصولا گیک شخصی است که به دنبال یادگیری در همه زمینه ها است و تلاش می کند اطلاعات خود را افزایش دهد، بطور مثال از ابزار و یا برنامه های متعددی استفاده می کند تا دید بهتری نسبت به نرم افزارها و قابلیت هایی که در اختیار کاربر قرار میدهند پیدا کند و کار خود را به بهترین نحو ممکن انجام دهد. اما در مقابل گیک افرادی هستند که تلاشی برای جستجو و یافتن ابزار جدیدی نمی کنند تا در مورد آنها اطلاعاتی کسب کنند و ترجیح می دهند از تعداد محدودی ابزار برای کار خود استفاده کنند به علتِ مدلِ رفتاری ای که این افراد در مورد کار با نرم افزار دارند، به آنها نرد می گویند. به تصور خیلی از گیک ها نرد ها ترس از استفاده و تجربه کار با ابزار های مختلف و جدید را دارند.

با توجه به حیاتی بودن مسئله امنیت در فضاهای مختلف سیستم های کامپیوتری و اینترنتی مانند شرکت های بزرگ که دارای سرویس های مختلفی هستند و حفاظت اطلاعات برای آنها بسیار ضروری است باید دقت بالایی در انتخاب نرم افزار داشته باشند. در کنار شرکت های بزرگ شبکه های مجازی هستند که اطلاعات کاربران را در اختیار دارند و باید بتوانند از حریم خصوصی افراد محافظت کنند. به همین دلیل افراد با تخصص بالا از نظر امنیتی را انتخاب می کنند تا بتوانند از نرم افزار های پیشرفته استفاده کنند. اکثر گیک ها به روش انجام این کار واقف هستند و بیشتر سعی می کنند از نرم افزار های پر قدرت استفاده کرده و یا برنامه ای را طراحی و پیاده سازی کنند که ملزومات یک ابزار امنیتی از همه لحاظ در آن رعایت شده باشد.

می توان به نکاتی اشاره کرد که یک گیک چه قابلیت هایی را برای نرم افزار خود در نظر می گیرد تا بتواند حداکثر امنیت را دارا باشد، برای مثال ساخت برنامه ای برای ورود کاربر به شبکه از الگوریتم رمزگذاری هایی با ضریب بالا استفاده می کند ، ابزاری برای تشخیص فایل های مخرب که می تواند از آلوده شدن سیستم جلوگیری کند و برنامه ای برای جلوگیری از ورود فرد یا افرادی که در سیستم تعریف نشده اند که آنها را شناسایی کرده و راه آنها را مسدود می کند.شرکت هایی در زمینه ساخت نرم افزار های امنیتی مانند آنتی ویروس و فایروال فعالیت می کنند و در تلاش هستند تا بهترین دستاورد های خود را که از آزمایشگاه های فوق پیشرفته استخراج میشود را در اختیار عموم قرار دهند. تعدادی از نرم افزار هایی که رتبه اول تا چهارم سایت (toptenreview) را دریافت کرده اند مورد بررسی قرار میدهیم که به شرح ذیل می باشند.

آنتی ویروس ها :



Bitdefender Antivirus Plus

شرکت بیت دیفندر در سال ۲۰۰۱ در کشور رومانی تاسیس شد و به یکی از بزرگترین تولیدکنندگان نرم افزار های امنیتی در دنیا تبدیل شد. بیت دیفندر از بدو تاسیس شرکت شروع به کشف و پاکسازی تهدیدات ویروس ها کرد و راه کارهایی برای شناسایی تهدیدات معرفی کرد، که یکی از این راه کار ها آنتی ویروس این شرکت می باشد .

این نرم افزار در سایت toptenreview با کسب نمره ۹,۹۸ توانست رتبه اول نرم افزارهای امنیتی را کسب کند و دلیل دریافت امتیاز بالا عبارت است از: محافظت از سیستم ، قابلیت اجرا ، قدرت انجام و پردازش ، سهولت اسکن، استفاده از منابع مربوطه ، جستجوی سریع اولیه معادل است با ۱,۷۶ دقیقه و در نهایت میانگین جستجو کامل آن ۶۰ دقیقه می باشد.



Kaspersky Anti-Virus

کسپراسکای یک شرکت روسی است که در سال ۱۹۹۷ تاسیس شد و همانند شرکت های بزرگ دیگر با استفاده از تکنولوژی های هوشمند برای شناسایی و پیشگری از ورود ویروس ها به سیستم های کامپیوتری به ساخت نرم افزار های مختلفی من جمله آنتی ویروس و فایروال پرداخت که دارای کاربران بسیاری زیادی می باشد. آخرین نسخه پایدار آنتی ویروس کسپراسکای در ۳ فوریه ۲۰۱۵ ارائه شده است. آنتی ویروس کسپراسکای در سایت toptenreview با کسب نمره ۹,۳۲ رتبه دوم ده آنتی ویروس برتر را دریافت کرده است. مقدار کمی از لحاظ محافظت، زمان جستجو و استفاده از منابع عقبتر می باشد اما سهولت جستجو میزان قابل مشاهده ای کمتر از بیت دیفندر می باشد.



McAfee AntiVirus Plus

شرکت مک آفی در سال ۱۹۸۷ به وسیله گروه امنیتی شرکت اینتل تاسیس شد که نام آن برگرفته از John McAfee است، کسی که در سال ۱۹۹۴ از شرکت استعفا داد. این شرکت هم مانند شرکت های امنیتی دیگر مسئول ساخت نرم افزار های برای شناسایی راه های نفوذ و تهدیدات امنیتی سیستم ها می باشد. این نرم افزار با کسب رتبه ۹,۲۸ در رده سوم محصولات آنتی ویروس در سایت ذکر شده قرار گرفته است.این نرم افزار در بعضی از قسمت های اجرا در سیستم مانند سرعت ، سهولت جستجو و ... ضعیفتر عمل کرده است.



Norton Security Deluxe 5

نورتون به وسیله شرکت Symantec توسعه یافت و در همان زمان مشغول به پیاده سازی روش های تست نفوذ و پیشگیری از حملات بدافزار ها شد. با پیشرفت تکنولوژی و بوجود آمدن ویروس و بد افزار های جدید، نورتون از استاندارد های پیشرفته برای توسعه نرم افزار ها استفاده کرد و همچنین نرم افزار آنتی ویروس خود را برای تمامی سیستم عامل ها مانند مایکروسافت ویندوز، مکینتاش، اندروید و iOS ارائه داد. این آنتی ویروس با کسب نمره ۹٫۰۵ چهارمین آنتی ویروس از ۱۰ مورد برتر موجود در لیست قرار گرفت.

@Badrinex







الگوریتم های رمز نگاری

رمزنگاری یا رمزگذاری یک فرآیند تبدیل یا ذخیره اطلاعات است که توسط یک الگوریتم خاص صورت می گیرد و هدف از این کار محافظت از اطلاعات است. دانش رمز نگاری به بررسی و شناخت و پیدا کردن یک راه مناسب برای ذخیره یا انتقال داده ها در مسیر هایی که نا امن است، میپردازد.

در هر رمز نگاری یک کلید الگوریتم وجود دارد که فقط در اختیار خود رمز نگار است و از آن برای رمز گشایی استفاده می کند، تعریف دیگر رمزنگاری فرآیندی است که در آن اطلاعات آشکار به اطلاعات رمز شده تبدیل میشوند. هدف از رمز نگاری ایجاد طرح ها و پروتکل هایی است که توسط آن ها بتوان حتی در محیط های نا امن با حفظ حریم داده ها به صورت کاملا امن ارتباط برقرار کرد.

رمزنگاری مدت های طولانی است که توسط دولت ها و گروه های نظامی برای برقرار کردن ارتباط امن و یا حتی مخفی استفاده می شود، اما در حال حاضر برای حفاظت امنیت داده ها استفاده می شود و لزوما در سیستم های نظامی کاربرد ندارد بلکه استفاده از آن در سیستم های خانگی نیز رواج دارد. از دیگر کاربرد های رمز نگاری می توان به تجارت الکترونیک اشاره کرد از جمله : مرجع صدور گواهی نامه/ کوکی ها / کارت های خرید /پروتکل های پرداخت و ...

به طور کلی می توان رمزنگاری را به دوسته کلی تقسیم کرد : ۱.رمزنگاری متقارن ۲.رمزنگاری نامتقارن

الگوریتم های متقارن به الگوریتم هایی گفته می شود که در آن از یک کلید هم برای رمز گشایی و هم برای رمز نگاری استفاده می شود و ساختاری ساده دارد ولی در الگوریتم های نا متقارن از یک زوج کلید استفاده می شود که عبارتند از کلید های خصوصی و کلید های عمومی .

کلید های خصوصی فقط در اختیارِ دارنده ی الگوریتم است و کلید های عمومی در اختیارِ کلیه ی کسانی که با دارنده آن در ارتباط اند است و امینت سیسیتم به محرمانه بودن کلید های خصوصی بستگی دارد.

از مزایای الگوریتم های متقارن می توان به ساده بودن آن (تنها با به اشترک گذاشتن کلید توسط کاربران میتوان عملیات را انجام داد)/ سریع بودن در عملیات/ کلید های کوتاه و عدم نیاز به منابع کامپیوتری زیاد اشاره کرد. در معایب این نوع از الگوریتم می توان نیاز به حفاظت کلید در دو طرف ارتباط/ نیاز به کانالی امن برای تبادل کلید/ تغییر کلید ها به صورت مداوم (معمولا در الگوریتم های موفق این نوع کلید ها به صورت مداوم تغییر می یابد) را نام برد و از مزایای الگوریتم های نا متقارن می توان گفت که حفاظت در این نوع الگوریتم آسان تر است و فقط باید از کلید های خصوصی حفاظت کرد/ کلید خصوصی و عمومی را می توان مدت زیادی بدون تغییر نگه داشت و می توان امکان احراز هویت فرستنده برای دیگران و عدم امکان انکار فرستنده فراهم کرد.

معایب این نوع الگوریتم عبارت اند از سرعت پایین در مقایسه با الگوریتم های متقارن/ بزرگ بودن کلید ها/ نیاز به منابع کاپیوتری زیاد و ضررات جبران نا پذیری در صورت فاش شدن کلید های خصوصی.

می توان گفت بیشترین کاربرد الگوریتم های متقارن در شبکه های کوچک با تعداد کاربر های کم است و در مقابل کاربرد الگوریتم های نا متقارن در شبکه های بزرگ با تعداد کاربر های زیاد است. در مورد مقایسه الگوریتم های رمز نگاری متقارن و نا متقارن بحث های زیادی شده ولی مقایسه این دو نوع رمز نگاری بدون در نظر گرفتن کاربرد آن ها (ارسال ایمیل/ رمز نگاری یک فایل/ برقرار کردن ارتباط متنی به صورت امن/ انتقال یک فایل و ...) نتیجه درستی حاصل نمی شود.اگر معیار مقایسه سرعت رمزنگاری باشد می توان گفت که الگوریتم های نا متقارن الگوریتم های بهتری هستند ولی اگر معیار امنیت بالا باشد الگوریتم های متقارن الگوریتم های بهتری هستند.در نهایت اینکه کدام یک از این الگوریتم ها با در نظر گرفتن تمام معیار ها بهتر هستند مشخص نشده. با این حال در مورد کاربرد این الگوریتم ها می توان گفت که در رمز نگاری های ساده که بیشتر سرعت مورد اهمیت است از الگوریتم های متقارن استفاده می شود و در رمز نگاری های پیچیده که موضوع مورد اهمیت امنیت است از الگوریتم های رمز نگاری نا متقارن استفاده می شود.

@THEnoneIDENtity



مصاحبه با یک گیک

بابز: برای شروع لطفا کمی خودتونو معرفی کنید و از سابقه گیکی خودتون برامون بگید.

حسین: من حسین حیدری هستم یک حامی و کاربر توزیع آرچ لینوکس و سعی در گسترش این توزیع دارم و از قدم‌هایی که برای توسعه و تبلیغ این توزیع برداشتم ایجاد کانال "آرچ لینوکس فارسی" و راه‌اندازی پروژه‌ی "آرچ تی‌وی" بوده.

بابز: اگر مایل باشی در مورد گنو/لینوکس بصورت کوتاه توضیحی ارائه بدی اونو چطور بیان میکنی؟

حسین: سیستم عاملی سریع، آزاد و انعطاف پذیر که به هر کسی اجازه می‌ده نسبت به سلیقه‌ی خودش در دنیای دیجیتال زندگی کنه.

بابز: چی باعث شده انگیزه ایجاد کانال آرچ لینوکس و همچنین تلویزیون آرچ در شما به وجود بیاد و هدفتون از این کار چی بوده؟

حسین: دلیل اول این بود که فکر می‌کنم باید منابع فارسی هم برای یادگیری مطالب مختلف وجود داشته باشه و از اونجایی که هیچ ویدیوکست فارسی درباره ی آرچ نبود، شروع کردم به ساخت ویدیوکست‌های آرچ لینوکس و در اولین قسمت نصب آرچو آموزش دادم تا بگم "آرچ لینوکس سخت نیست" و ترس از نصب و پیکربندی آرچ یک ترس مسخره است. دلیل ساخت کانال‌هم گسترش دادن کاربران آرچ لینوکس بود که تا الان موفق بوده :)

بابز: کمی در مورد آرچ لینوکس توضیح بدین . در این چند ماه گذشته خیلی در مورد آرچ لینوکس در کانالها و گروه های تلگرامی و یا وبلاگهای مختلف روی اینترنت صحبت شده. میشه کمی ما رو با آرچ لینوکس و تفاوتهای اون با دیگر انواع لینوکس آشنا کنید؟

حسین: تفاوت آرچ لینوکس با دیگر توزیع‌ها در فلسفه‌ی اونه, آرچ با هدف سبکی و سادگی اومده و از پایه همه چیزو کاربر انتخاب، نصب و پیکربندی می‌کنه و یا از دیگر سیاست‌های آرچ میشه به غلطان بودنش اشاره کرد که همیشه آخرین نسخه از یک بسته رو در اختیار کاربر قرار می‌ده و به همین دلیل همیشه سیستم به روز خواهد بود.

بابز: چرا در چند وقت گذشته استقبال جامعه کاربران ایرانی از آرچ زیاد شده و افراد بیشتری نسبت به قبل به سمت این توزیع جذب میشن؟

حسین: این به دلیل راه اندازی انجمن فارسی آرچ یعنی "http://archusers.ir" و همینطور پروژه‌ی آرچ تی وی بوده تا کاربران بیشتر با آرچ یا مشتقاتش آشنا بشن و بیشتر به سمت این توزیع حرکت کنن, تلاش دوستان برای ترجمه‌ی ویکی آرچ انگلیسی به فارسی هم تاثیر زیادی به جذب کاربرانِ فارسی زبان داشته تا اونها بتونن به زبان مادری درباره‌ی آرچ لینوکس مطالعه کنند.

بابز: کمی بیشتر برامون از تلویزیون آرچ بگید و اینکه چه موضوعاتی رو تا حالا پوشش دادید و چه برنامه ای برای آینده در دست تهیه دارید؟

حسین: خب می‌تونم بگم آرچ تی وی یکی از بهترین تجربه های زندگی من بوده، تا الان راجع به نصب آرچ, پیکربندی پکمن کانف، فلگ‌های پکمن, نصب مانجارو با خط فرمان و با رابط گرافیکی و غیره مطالبی تهیه شده و در آینده هم قصد ساخت ویدیو درباره‌ی وب سرور آپاچی، وارد کردن ماژول‌های php۷ در اون یا پایگاه داده، تور، فایروال و ... رو دارم.

بابز : آیا در این پروژه تنها هستید یا کسانی هم به شما کمک میکنن؟ آیا افراد دیگه ای هم میتوانند به این پروژه اضافه شوند یا خیر؟

حسین: فعلا تنها هستم ولی بقیه افراد هم می‌تونن شرکت کنن, و اگه تعداد زیاد شد شاید حتی یه سایت هم براش درست کردیم!

بابز: خوب کمی در مورد خودتون و رفتارهای گیکیتون بگید. از چه زمانی با دنیایی تکنولوژی آشنا شدید و تمرکزتون روی چه مسائلی در زمینه تکنولوژی بوده و هست؟

حسین: بیشتر سعی می‌کنم با چیزهایی کار کنم که منو به چالش می‌کشن مانند آرچ لینوکس, دوست دارم خودم همه چیز را کانفیگ کنم و بدونم هر پوسته‌ای که نوشته میشم, هسته اش چطوری کار می‌کنه و فقط نمی خوام کارمو راه‌بندازم برای مثال سعی کردم با MySQL در خط فرمان کار کنم تا PHPMyAdmin, از ۵ سالگی با دنیای تکنولوژی آشنا شدم و خب اون موقع ویندوز XP بود, همه‌ی تمرکز من فعلا بر روی برنامه نویسی و گنو/لینوکس هست و قصد فعالیت در شبکه در آینده را هم دارم هر چند هنوز وارد دنیایی شبکه نشدم.

بابز: با تشکر از وقتی که برای این مصاحبه گذاشتید بعنوان سوال آخر چه پیشنهادی به کسانی که میخواهند در دنیای تکنولوژی بصورت تخصصی وارد بشن دارید؟

حسین: IT دنیای وسیعیه و هر کس در قسمتی از اون تخصص داره اما به عنوان کسی که بیشتر روی گنو/لینوکس تمرکز داره باید بگم اگر کسی از ویندوز استفاده می‌کنه اونو رها کنه و به دنیای گنو/لینوکس اضافه بشه (فارغ از توزیع خاصی)

@BOBZBOBZ



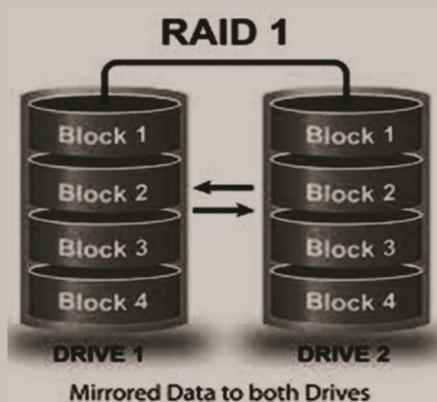
گیـــــک و شبـــــــکه

امروزه با پیشرفت تکنولوژی و ورود کامپیوتر به تمامی عرصه ها، نقش پررنگ شبکه های رایانه ای در سازمانها و شرکتها بر هیچکس پوشیده نیست. شاید از دید کاربران عادی، شبکه فقط متصل کردن چند سیستم و در نهایت به اشتراک گذاری منابع باشد ولی در واقع چگونگی اتصال سیستم ها به یکدیگر، نحوه ی ذخیره سازی دیتاها، سیاست های حفاظت از اطلاعات، چگونگی مدیریت کاربران، داشتن سیاست هایی برای پشتیبان گیری از اطلاعات و ... مواردی هستند که در طراحی هر شبکه ای، متخصصان باید بدان توجه داشته باشند.

یک طراح شبکه، برای طراحی ساختار شبکه، قبل از هرچیز باید نیازهای سازمان مربوطه را بسنجد، و سپس با توجه به نیاز سازمان و امکانات موجود اقدام به طرح ریزی و پیاده سازیِ طرح نماید. برای داشتنِ ساختار درست موارد خیلی زیادی هستند که باید رعایت شوند. در ادامه به چند مورد از کارهایی که باید صورت پذیرد اشاره ای خواهیم داشت.

RAID

Raid مخفف عبارت Redundant Array of Inexpensive Disks و تکنولوژی برای ترکیب چندین هارد دیسک به یک واحد، با هدف افزایش امنیت، سرعت و کارایی دیسک های ذخیره سازی می باشد. Raid انواع مختلفی دارد که برخی از آنها به صورت رایگان برای پیکربندی فعال می باشند و برخی دیگر نیاز به لایسنس دارند. بسته به اینکه ما در ساختار خود به سرعت نیاز داریم یا اینکه امنیت برای ما در الویت بالاتری قرار دارد و یا تلفیقی از امنیت و سرعت مورد نیاز سازمان می باشد، میتوان Raid مورد نظر را انتخاب کرد.



Virtualization

قطعا یکی از مهمترین مواردی که هر کسی در طراحی شبکه باید به آن توجه ویژه ای داشته باشد استفاده بهینه از سخت افزار و تقسیم سخت افزار برای وظایف خاص می باشد . مجازی سازی تکنولوژی است که برای این کار به کمک ما می آید و با متمرکز سازی و استفاده از بیشترین ظرفیت تجهیزات سخت افزاری، به سازمانها در کاهش هزینه کمک شایانی می کند. در واقع با مجازی سازی این امکان فراهم می شود که سرورهای متعددی بر روی یک سرور فیزیکی داشته باشیم و هر ماشین مجازی را برای سرویس خاصی در نظر بگیریم. این امر این امکان را به ما میدهد که اگر یکی از سرورهای ما به هر دلیلی از سرویس دهی خارج شد سایر سرورها به صورت مستقل به فعالیت خود بدون اخلال ادامه دهند که باعث افزایش امنیت می گردد.

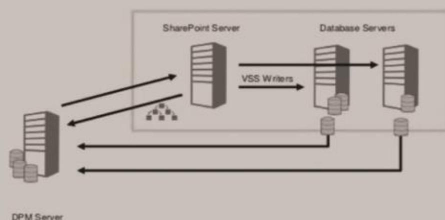
Automatic Backup

پراهمیت ترین بخش هر سازمانی، اطلاعات آن سازمان می باشد. همواره حفاظت از اطلاعات و سیستم ها به دلیل رشد روز افزون آنها در سازمان و پیچیدگی های خاص خود سخت و طاقت فرسا است چرا که یکی از اساسی ترین مشکل و ریسک بزرگی که سازمان ها با آن مواجه هستند خطرات ناشی از انهدام داده ها می باشد.

به همین منظور هر سازمان نیاز به روش ها و استاندارد هایی دارد تا بتواند از تمامی اطلاعات حیاتی خود پشتیبان گرفته و همچنین هنگام از بین رفتن اطلاعات در حداقل زمان ممکن آن را بازیابی کرده و سازمان را در مسیر عادی خود قرار دهد. برای تهیه بک آپ از تمامی اطلاعات حیاتی سازمان این کار باید به صورت اتوماتیک صورت پذیرد تا احتمال هرگونه فراموشی یا سهل انگاشتن در تهیه پشتیبان را از بین برود. از Symantec nova Backup، Veam Backup، Backup Exet، Argentum Backup میتوان به عنوان بهترین نرم افزارهای پشتیبان گیری نام برد.

DPM: Database Protection Manager

سیستمی است که به ما اجازه میدهد بک آپ ها را از مبدا به یک نقطه دیگر منتقل نماییم. DPM میتواند هر دو نوعِ Full Backup و Incremental Backup را تهیه نماید. با داشتنِ DPM اگر تحت هر شرایطی Backup های اولیه ما غیر قابل دسترس باشند و یا از بین بروند، میتوان از Backup های ثانویه ی ذخیره شده بر روی DPM استفاده نمود. در واقع DPM نیز یکی دیگر از سیاست هایی است که امنیت داده های سازمان را به طور قابل ملاحظه ای افزایش میدهد. DPM را میتوان علاوه بر سرورهای سخت افزاری، روی Virtual Machine نیز نصب و پیکربندی کرد.



@mansourebrahimi

سیستم عاملِ اَمنه؟؟



مهمترین برنامه نصب شده در یک کامپیوتر ، سیستم عامل است. به عبارت دیگر سیستم عامل نقش روح را در پیکر سخت افزاری کامپیوتر ایفا می کند. در انتخاب سیستم عامل باید کلیه ابعاد فنی کامپیوتر و فناوری و امنیتی را در نظر گرفت.

مهمترین دارایی کشورها ، سازمان ها و حتی اشخاص اطلاعات است و این نکته نیز بسیار حائز اهمیت است که بدون امنیتِ اطلاعات، امنیت سیاسی ، اقتصادی و نظامی نیز میسر نخواهد بود.

گسترش شبکه های کامپیوتری در سطح دنیا و امکان ارتباط همه کامپیوترها با یکدیگر، پتانسیل نفوذ به هر کامپیوتر را در هر جای دنیا فراهم کرده است. وجود آسیب پذیری در سیستم عامل، راه نفوذ راحت تری برای Attackerها فراهم میکند، از این رو امنیت سیستم عامل مهمترین مولفه در امنیت اطلاعات و شبکه های کامپیوتری می باشد.

کمتر گیکی هست که در مورد حملات به سیستم عامل ها و مشکلات امنیتی آن نداند. مشکلاتی از قبیل Trojan ، **Phishing** ، **Sniffing**ها ، ویروس ها ، Malwareها و ....

هر کاربری با توجه به نوع استفاده خود نسبت به انتخاب سیستم عامل اقدام می کند، هر سیستم عامل ویژگی ها، مزایا و محدودیت های مختص به خود را دارا می باشد، در این رابطه می توان به متداولترین سیستم عامل های موجود اشاره نمود:

ویندوز (Windows): ویندوز که دارای نسخه های متعددی است متداولترین سیستم عامل استفاده شده توسط کاربران می باشد. این سیستم عامل توسط شرکت مایکروسافت ارائه شده و دارای یک رابط گرافیکی است که استفاده از آن را برای اکثر کاربران راحت تر می نماید (نسبت به سیستم های عاملی که دارای رابط کاربری مبتنی بر متن می باشند).

Mac OS: سیستم عامل فوق توسط شرکت اپل ارائه شده است و از آن بر روی کامپیوتر های تولید خود (که آن را مکینتاش می نامد) استفاده میکند.

لینوکس و سایر سیستم عامل های مبتنی بر یونیکس:
لینوکس و سایر سیستم های عاملی که از یونیکس مشتق شده اند ، عمدتا استفاده از آن ها توسط کاربران معمولی مشکل بوده و به دانش و یا مهارت خاصی نیاز دارد. همین موضوع یکی از دلایل اصلی برای عدم گسترش عمومی آن ها محسوب می شود. نسخه هایی نیز از سیستم عامل فوق پیاده سازی شده تا کاربران معمولی نیز بتوانند به سادگی از آن ها استفاده نمایند(مانند Ubuntu,Mint,...).

جدا از اینکه سیستم عامل انتخابی برای نصب بر روی کامپیوتر چیست ، هر سیستم عامل برای امن ماندن به مواردی نیاز دارد. ابتدایی ترین نیازمندیهای امنیتی یک سیستم عامل به شرح زیر است:



Firewall: سامانه نظارت و مراقبت امنیتی می باشد ، در کل به نرم افزارها یا سخت افزارهایی گفته می‌شود که از دسترسی‌های غیرمجاز به کامپیوتر فرد در یک شبکه یا اینترنت جلوگیری کرده و داده‌های ورودی و خروجی را کنترل می‌کند. درواقع کار فایروال بسیار شبیه به در خانه شماست. کسانی که مجوز ورود را دارند می‌توانند وارد خانه شوند و برعکس کسانی که حق ورود به خانه را ندارند، نمی‌توانند به آن وارد شوند (با این تفاوت که معمولاً در فایروال‌ها هر دو جهت ورودی و خروجی کنترل می‌شود). یعنی فایروال به عنوان یک لایه امنیتی ، داده‌ها و ارتباطات را فیلتر می‌کند.

Passwords: یک عبارت متوالی رمزی است که فرد برای بدست آوردن جواز دسترسی به اطلاعات باید وارد کند و برای شناسایی و اهداف امنیتی در یک نظام کامپیوتری بکار میرود. Password در امنیت اطلاعات از نوع Defensive می باشد ، یعنی یک اقدام واکنشی است برای گرفتن مجوز دسترسی به اطلاعات که به محض درخواست برای دسترسی به اطلاعات، بکار میرود.

Biometrics(زیست سنجی): در کل زیست سنجی ، علم و فناوری سنجش و تحلیل داده های زیستی است. در فناوری اطلاعات، زیست سنجی معمولا به فناوری هایی برای سنجش و تحلیل ویژگی های بدن انسان (مانند اثر انگشت ، قرنیه ، الگوی صدا و ...) به منظور تعیین اعتبار اشاره دارد. یکی از ویژگی های ذاتی علم زیست سنجی این است که کاربر باید با یک الگوی مرجع مقایسه شود. شاخصه های زیستی را میتوان جایگزین کارت هوشمند نمود و کاربران میتوانند هم از کارت هوشمند و هم از اثر انگشت یا چهره خود برای تعیین اعتبار در امور بازرگانی، بانک ها یا ارتباط تلفنی استفاده نمایند. **Biometric** هم از نوع **Defensive** می باشد.

Antivirus: با ورود کامپیوتر به دنیای کنونی ، Virus ها، Trojanها ، Wormها و .... برای اهداف خاصی متولد شدند. با تولد این بد افزارها، مهندسان امنیت اطلاعات نیز بر آن شدند که به مبارزه با آن ها به پا خیزند و به جهت رفع آن برآیند. **Windows** بدلیل استفاده عموم مردم بیشترین نیاز را به **Anti-virus** دارد، ولی لینوکس و **Mac** نیز از این قاعده مستثنی نیستند. یکی از مهمترین پارامترها برای داشتن یک سیستم عامل امن داشتن یک **Antivirus** به روز و مطمئن می باشد.

رفع نقاط آسیب پذیری: یکی دیگر از اقدامات برای داشتن یک سیستم عامل امن ، رفع نقاط آسیب پذیری است ، این بدان معنا نیست که فرد استفاده کننده خود به دنبال نقاط آسیب پذیری در سیستم عامل خود بگردد. فقط نیاز است سیستم عامل خود را Update یا به اصطلاح بروز نگاه دارد. این بروز رسانی برای پر کردن Bugها و بستن Backdoorهاست که مورد استفاده مهاجمین و سارقان اطلاعات است.

افزایش دانش عمومی کاربران (مهمترین قسمت امنیت سیستم عامل): افزایش دانش عمومی کاربران در جهت استفاده از سیستم عامل یکی از مهمترین اقدامات برای امن نگاه داشتن سیستم عامل است، بطوریکه اکنون در سازمانها آموزش کارکنان یکی از مهمترین استانداردهای امنیتی می باشد. بدون در نظر گرفتن عوامل انسانی امنیت در سیستم عامل معنا و مفهوم خاصی ندارد و مهمترین عامل در خطرات امنیتی سیستم عامل ،عامل انسانی و کمبود دانش اوست.



همانطور که پیش تر گفته شد ، اطلاعات مهمترین دارایی هر شخص ، سازمان و یا کشور است. در صورت عدم توجه به هرگونه موارد اشاره شده ، امن ماندن سیستم عامل ، امری دور از ذهن می باشد و شاید زمانی فرا برسد که ما قادر به پرداخت تاوان چیزی که از دست داده ایم، نباشیم.

@An0nym0u3

سخت افزار چیست؟

سخت افزار چیست؟

سخت افزار یکی از شاخه های مهم علوم کامپیوتر محسوب می شود و به کلیه ی اجزا و قطعات کامپیوتر که به طور فیزیکی وجود دارند و می توان آنها را لمس کرد، گفته می شود. آشنایی با سخت افزار و نحوه ی کارکرد هر کدام از قطعات ،کاربران را در استفاده ی هرچه بهتر از کامپیوتر کمک خواهد کرد.همچنین می توانند از همه ی پتانسیل ها و قابلیت های کامپیوتر خود به آسانی بهره بگیرند. تولید و ساخت قطعات مهم و اصلی کامپیوتر منحصر به شرکت های خاصی است که اکثر آنها در کشورهای توسعه یافته مانند آمریکا ،چین ژاپن و... فعالیت دارند.سخت افزار نیز مانند دیگر علوم کامپیوتری روز به روز دچار تغییر و دگرگونی می شود .در این بین بعضی از تکنولوژی های قدیمی تر از رده خارج می شود و جای خود را به فن آوری جدیدتر می دهد یا یک فن آوری قدیمی به روز شده و قابلیت هایی به آن افزوده خواهد شد.

امنیت در سخت افزار

سخت افزارهای یک رایانه که به عنوان اجزای ورودی و خروجی مورد استفاده واقع می شوند جزء ابزارهایی هستند که نفوذگران ،نرم افزارهای مخرب خود را از آن طریق در رایانه وارد می کنند.این مجموعه قطعات می توانند از درایورهای انواع CD ها و یا انواع کارت هایی که به رایانه اضافه می شوند و انواع پورت های رایانه وارد شبکه ما شوند.

هدف از ایجاد امنیت

وظیفه اصلی این دستگاه های سخت افزاری در شبکه ،کنترل بسته های عبوری و بررسی آنها با قوانین و تنظیماتی که در آنها انجام شده به منظور مسدود نمودن دسترسی و یا باز نمودن مسیر به داخل یا خارج از شبکه به جهت برقراری امنیت اطلاعات و جلوگیری از افشای اطلاعات می باشد.از وظایف دیگر آنها می توان به:جلوگیری از ایجاد اختلال در ارائه سرویس های شبکه،جلوگیری از بروز حملات مختلف به شبکه،جلوگیری از خروج اطلاعات از شبکه،جلوگیری از ورود افراد غیرمجاز و دسترسی پیداکردن به سیستم ها اشاره کرد.

معرفی سخت افزار های امنیتی

۱) Cyberoam

امروزه با بالا رفتن تعداد کاربران اینترنت و آشنایی آنها با نرم افزارهای نفوذ به شبکه های کامپیوتری و همچنین با رشد میزان اطلاعات موجود بر روی سرورهای سازمانها، نیاز به نظارت بر امنیت شبکه های کامپیوتری اهمیت بسزایی پیدا کرده است. عدم آشنایی بسیاری از کاربران و پرسنل سازمانها، به نفوذگران کمک می کند تا به راحتی وارد یک شبکه کامپیوتری شده و از داخل آن به اطلاعات محرمانه دست پیدا کنند یا اینکه به اعمال خرابکارانه بپردازند.

محصولات امنیتی یکپارچه Cyberoam به منظور برطرف کردن نیازمندی‌های امنیتی شبکه‌های کوچک، متوسط و بزرگ ارائه شده است. با توجه به توسعه کاربرد شبکه و خدمات مبتنی بر آن در سازمان‌ها، نیاز به راهکارهای امنیتی جامع و یکپارچه بیش از پیش احساس می‌شود. شرکت سایبروم محصول جامع امنیتی Cyberoam UTM را برای کلیه نیازهای سازمان شامل مدیریت امنیت درگاه شبکه، مانیتورینگ متمرکز ارائه کرده است. در این محصول چندین ویژگی برای تامین امنیت فراگیر و افزایش کارایی، بر روی یک دستگاه واحد ارائه شده است. ویژگی متمایز کننده دستگاه امنیتی یکپارچه Cyberoam با دیگر تجهیزات، استفاده از مشخصات کاربر و گروه کاری به منظور احراز هویت، اعمال محدودیت‌های استفاده از اینترنت و اعمال سیاست‌های کنترل دسترسی می‌باشد. تجهیزات امنیتی یکپارچه Cyberoam موفق به کسب EAL۴+ (Evaluation Assurance Level ۴+) بالاترین سطح گواهینامه بین‌المللی استانداردهای امنیتی و فناوری اطلاعات (ISO/IEC ۱۵۴۰۸) در سپتامبر ۲۰۱۳ گردید. همچنین این محصول دارای گواهینامه سطح ۵ (UTM LEVEL ۵) از سوی موسسه معتبر Check Mark و همچنین اخذ تائیدیه لابراتوار ICSA به عنوان سیستم‌های مدیریت یکپارچه تهدیدات اینترنتی مبتنی بر شناسه کاربر می‌باشد.

ویژگی ها:

- متوقف نمودن حملات DoS و DDoS برای جلوگیری از قطع موقت یا دائمی و یا تعلیق خدمات میزبان متصل به اینترنت.
- دیواره آتش با قابلیت ایجاد سیاست‌های کنترل دسترسی بر اساس شناسه کاربر، آدرس IP، MAC و سرویس‌های مبدا و مقصد.
- پشتیبانی از روش‌های رمزنگاری شامل DES، ۳DES، Blowfish، Twofish، AES و Serpent.
- تشخیص و جلوگیری از ورود ویروس، کرم، تروجان و جاسوس افزار.



۲) Cisco ASA

امنیت شبکه برای سازمان هایی که قادر نیستند تجهیزات مجزا نظیر AntiVirus,IPS,Firewall و سرویس های VPN را خریداری کنند یک چالش جدی است.

ASA مخفف Adaptive Security Appliance می باشد که چندین قابلیت را باهم ترکیب کرده است از جمله قابلیت‌های فایروال، آنتی ویروس، ممانعت نفوذ و VPN را دارد و اگر حمله‌ای در شبکه رخ دهد، قبل از اینکه حمله در تمام شبکه پخش شود، به صورت خودکار برای متوقف کردن آن مبادرت می‌کند. ASA به عنوان وسیله‌ای کاملا ارزشمند و انعطاف پذیر است که به عنوان راه حل امنیتی برای شبکه‌های کوچک و بزرگ استفاده می‌شود. اما ASA فقط یک فایروال نیست بلکه ترکیبی از فایروال، آنتی ویروس، ممانعت نفوذ و VPN است.

بنابراین Cisco ASA نه تنها فایروال است بلکه موارد زیر را نیز شامل میشود:

- Antivirus
- Antispam
- IDS/IPS engine
- VPN device
- SSL device
- Content inspection

Cisco ASA یکی از بزرگترین بازارهای سخت افزارهای فایروال را دارد و رقبایی مانند Juniper Netscreen ، Check-point، SonicWall و WatchGuard و غیره دارد. سری Cisco ASA ۵۵۰۰ در واقع سرویس های جامع امنیت شبکه را ارائه می دهد. به منظور رسیدن به فایروال مقاوم، هر نوع سیستم‌های تجارتی با هر سایزی نیاز به سرویس‌های کامل امنیتی دارند که شامل VPN ، محتوای امنیتی، دسترسی از راه دور، ممانعت نفوذ و ارتباطات یکپارچه می‌باشد.

ویژگی ها:

- سیستم IPS جامع وکارا همراه با Cisco Global Correla-tion ارائه می‌دهد
- VPN با کارایی بالا و دسترسی از راه دور
- آنتی ویروس اختیاری، آنتی اسپم، آنتی فیشینگ، بلاک کردن و فیلتر کردن URL و کنترل محتوا

۳)Juniper

به منظور مقابله با حملات لایه شبکه ،تجهیزات Juniper از یک روش پویا و موثر در پالایش بسته های داده استفاده می کنند . در این روش که بازرسی حالتمند نام دارد اطلاعات گردآوری شده از سرآیند بسته ها با اطلاعات موجود ازSessionمربوطه مقایسه شده و در صورت مغایرت،بسته پذیرفته نمی شود .

ارتباط ایمن و قابل اعتماد در اتصالات WANنیز نقش مهمی در امنیت لایه شبکه دارد . با ایجاد شبکه های مستحکم خصوصی مجازی ،کاربران و دفاتر راه دور امکان برقراری ارتباط امن و مطمئن با داده ها و برنامه های متمرکز از طریق یک شبکه عمومی نظیر اینترنت فراهم می گردد . امکان ایجاد و مدیریت VPNدر تجهیزات Juniperبراحتی فراهم می باشد .

برای مقابله با حملات لایه کاربرد،Juniperسامانه پیشگیری از نفوذ را در محصولات خود گنجانده است . برای سایتهای مرکزی و مراکز داده که قابلیت گذردهی بالایی دارند ،شرکت Juniper امکانات IDPرا در سری محصولات ISGتعبیه کرده است . قدرت پردازش بالا و بی نظیر،امکانات قطعه بندی شبکه و پشتیبانی بیش از ۶۰ پروتکل،محصولات ISGرا بهترین انتخاب برای محافظت شبکه های سریع و مراکز داده در مقابل نفوذ و گسترش تهدیدات لایه کاربرد،نموده است . دستگاه ISGبا ماجول IDP، با استفاده از مکانیزم های شناسایی چندگانه تحلیل عمیقی از پروتکل و محتوا در لایه کاربرد انجام می دهد و شبکه را در برابر حملات ZERO-DAYمقاوم می سازد .

در دیگر محصولات شرکت Juniperنیز امکانات سامانه پیشگیری از نفوذ به نوعی تعبیه شده است . فناوری Deep Inspectionفقط دو روش از هشت روشی را که در محصولات IDPموجود است ،بکار می برد . فایروال هایی که IDPدر آنها فعال می باشد درک عمیق تری از ترافیک شبکه در لایه کاربرد دارند و برای لبه یا پیرامون شبکه مناسبتر می باشند و حملات لایه کاربرد را قبل از سرایت به شبکه و وارد کردن خسارت،متوقف می کنند.

ویژگی ها:

- این محصولات علاوه بر این که امکانات فایروال و VPNرا دارند ،امکان محافظت در برابر ویروس های موجود در پست الکترونیکی و صفحات WEBرا با بررسی و پویش پروتکل های IMAP,SMTP,FT-HTTP,P,POP۳فراهم می کنند سامانه ضد ویروس این تجهیزات توانایی پویش فایلهای فشرده را تا چندین لایه نیز دارند .، کارکنانی که به سایتهای نامناسب دسترسی پیدا می کنند ،شبکه سازمان را با ورود نرم افزاری مخرب به مخاطره می اندازند . تجهیزات یکپارچه شرکت Juniperاین امکان را برای سازمان بوجود می آورد که بتوانند یک خط مشی استفاده مناسب از وب را تدوین و اعمال کنند .
- شرکت Juniper Networksبا همکای Symantecراه حل جلوگیری از نامه های ناخواسته و حملات Phishingرا بر روی دستگاه های خانواده NS-۲۵,SSG,NS-HSC,NS-SGT,NSوNS-۵۰تعبیه کرده است . این ویژگی با محدود کردن ورود هرزنامه و مخاطرات همراه آن در اولین لایه دفاعی شبکه به شرکتهای کوچک و متوسط در ایمن سازی نامه های الکترونیکی کمک می کند .
- فناوری JSRP جونیپر پایداری و در دسترس پذیری بالا را برای شبکه هایی که فایروال های سری SRX یا ISG در آن تعبیه شده است ، به ارمغان می آورد .

۴)fortigate

شرکت فورتی نت یکی از بزرگترین تولید کنندگان تجهیزات امنیت شبکه در کل دنیا می باشد و همچنین جزء اولین شرکت هایی ست که تجهیزات مدیریت یکپارچه تهدیدات (UTM) ارائه می دهد. در ماه می سال ۲۰۰۲که اولین محصول شرکت فورتی نت بنام fortigate معرفی شد محصولات پرفروش fortigate پیشرفت قابل توجهی را بدست آوردند. محصولات ارائه شده در عین سادگی با قابلیت ارائه بالاترین کارائی در مقابل تهدیدات امنیتی طراحی شده اند. لازم به ذکر است این محصولات با رابط کاربری ساده (GUI) امکان تنظیمات و تغییرات را برای کارشناسان شبکه به سادگی فراهم می کنند.

شرکت فورتی نت در بازار مدیریت یکپارچه حملات (UTM) پیشگام بوده و برترین تجهیزات امنیت شبکه را که شامل فایروال ، آنتی ویروس ، VPN ، سیستم جلوگیری از نفوذ ، جلوگیری از هرزنامه ها ، فیلترکردن سایتها و مدیریت ترافیک می شوند، در راهکارهای امنیتی شبکه ارائه داده است.

محصولات fortigate که شامل سیستمهای مدیریت یکپارچه حملات می باشند که سطح امنیت بالایی را با ترکیب بهترین و برترین برنامه های کاربردی شامل فایروال ، آنتی ویروس ، سیستم جلوگیری از نفوذ ، VPN، امکان وب فیلترینگ ، جلوگیری از هرزنامه ها و مدیریت ترافیک شبکه ارائه می دهند.

تجهیزات fortigate دارای گواهینامه های معتبری همچون +EAL۴ و NSS بوده و همچنین تنها سیستمهای امنیتی هستند که چندین بار از ICSA Lab تائیدیه گرفته اند. سیستمهای fortigate یک لایه بحرانی بلادرنگ، در حفاظت آنتی ویروس بر مبنای شبکه اضافه می کنند که نرم افزارهای آنتی ویروس را تکمیل میکنند و بدون اینکه طراحی را هزینه بر و کارآیی را پایین بیاورند.

ویژگی ها:

- با کمک این محصول خواهید توانست با ایجاد فایروال و پیاده سازی پروفایل های امنیتی شبکه خود را از نفوذ ویروسها و حملات حفظ نموده و توانایی فیلترینگ محتویات وب و شناسایی هرزنامه ها را هم داشته باشید.
- کنترل محتویات ترافیک و Application ها را نیز می توان با این دستگاه انجام داد.

و در آخر اینکه در اثر بی توجهی به امنیت در شبکه موجب نفوذ به شبکه و از بین رفتن اطلاعات محرمانه ، از کار انداختن سرورها و اشغال شدن پهنای باند ، تخریب اطلاعات موجود و نرم افزارها می شویم و با توجه به نا امن بودن شبکه های موجود و گسترش روز افزون ویروسها و حملات کامپیوتری و همچنین گسترش و افزایش اطلاعات با ارزش برروی شبکه ها، وجود سخت افزارهای امنیتی جهت تمام شبکه های کامپیوتری داخل سازمانها الزامی می باشد.

@Mehnaty



گیک و مجازی سازی (امنیت)

اگر در زمینه فناوری اطلاعات فعالیت داشته باشید، قطعا در سال های اخیر نام مجازی سازی را بارها و بارها شنیده‌اید و از پیشرفت روز افزون این تکنولوژی در دنیای فناوری اطلاعات مطلع هستید.

اما چه عواملی باعث این پیشرفت شگفت انگیز شده است؟ مجازی سازی باعث استفاده بهینه از سخت افزارها و مدیریت راحت تر و انعطاف پذیرتر سرورهای فیزیکی و سیستم عامل شده‌است. همان طور که می دانید سخت افزارهای پیشرفته دارای هزینه های بسیار بالایی هستند و تمامی مراکز IT سراسر دنیا سعی در کاهش هزینه‌ها و استفاده بهینه از منابع خود را دارند. مجازی سازی باعث افزایش اطمینان و امنیت سیستم‌ها و کاهش پیچیدگی عملیاتی می‌شود.



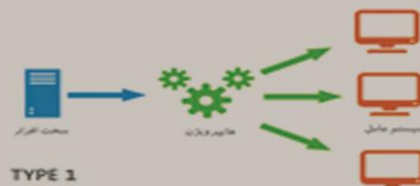
هایپروایزر(Hypervisor) چیست و چه کاربردی دارد ؟

یک هایپروایزر (Hypervisor) یکی از دو روش برای مجازی سازی یک محیط محاسباتی است، منظور ما از virtualize ، تقسیم منابع مانند CPU , RAM از یک محیط محاسبات فیزیکی (شناخته شده به عنوان سرور اصلی میزبان) به چند ماشین مجازی کوچکتر (شناخته شده به عنوان سیستم عامل مهمان) می باشد. هر مهمان می تواند سیستم عامل مورد نیاز خود را نصب کند و هر ماشین مجازی RAM و CPU خود را دارد ، در واقع سرور مجازی درست مانند یک سرور فیزیکی رفتار می کند، این امکان نیازمند پشتیبانی قابلیتی به نام VT-x در سی پی یو های اینتل و AMD-V در سی پی یو های AMD است.

یکی از وظایف کلیدی که Hypervisor فراهم می کند جداسازی است، این به این معنی است که یک مهمان امکان دسترسی به سرور میزبان و همچنین دسترسی به سایر مهمان های (ماشین های مجازی) ایجاد شده در سرور ندارد و رفتار های سرور مهمان روی آنها تاثیری نداشته باشد، حتی اگر ماشین مهمان با مشکلاتی مانند کرش شدن مواجه شود. بنابراین Hypervisor باید به دقت مانند یک سخت افزار ماشین فیزیکی عمل کند و از دسترسی مهمان به سخت افزار واقعی جلوگیری کند، از آنجایی که این عمل به شدت سرعت را کاهش می دهد از یک روش paravirtualized یا PV drivers استفاده می شود. این امکان تمام سخت افزار ها را به صورت مجازی در اختیار ماشین مجازی قرار می‌دهد و درایور های آن توسط Hypervisor دریافت می شود، با استفاده از این روش سرعت بالا می رود و همچنین امکان دسترسی مستقیم به سخت افزارهای اصلی سرور و کنترل آنها توسط مهمان دیگر وجود ندارد.

Hypervisors دو نوع است Type ۱ و Type ۲

Type ۱ : در این نوع، Hypervisors به طور مستقیم برای کنترل سخت افزار و سیستم عامل های مهمان اجرا می‌شود. بنابراین مجازی ساز های VMware ESXi و Xen از نوع Type ۱ می باشد. تصویر زیر مثالی type ۱ است :



Type۲: دراین نوع، Hypervisors در داخل یک سیستم عامل اجرا می شود و پس از آن سیستم عامل های مهمان ایجاد می شود. سیستم های مجازی ساز دسکتاپ اغلب از این روش استفاده می کنند. بنابراین مجازی ساز های OpenVZ و KVM از نوع Type ۲ هستند.تصویر زیر مثالی type ۲ است



با تصاویر بالا نتیجه می گیریم Hypervisors تایپ ۱ بهتر از تایپ ۲ است زیرا در تایپ ۱ Hypervisors هنگام دسترسی به منابع فیزیکی از سیستم عامل میزبان استفاده نمی شود. پیدا کردن نوع Hypervisors کاری بسیار ساده است ، برای مثال مجازی ساز که به عنوان یک پردازش در سیستم عامل میزبان لینوکس نصب می شود از نوع TYPE-۲ است. در واقع فرآیند راه اندازی صرفا دسترسی به تعداد محدودی منابع از طریق سیستم عامل میزبان و بسیاری از وظایف حساس توسط ماژول کرنل انجام می شود که دسترسی مستقیم به سخت افزار را دارد. شرکت Vmware یکی از بزرگترین و پیشرفته ترین شرکت هایی در دنیا است که خدمات مجازی سازی را ارئه می‌دهد و بسیاری از سازمان‌ها و مراکز IT از محصولات شرکت Vmware جهت مجازی شبکه‌های خود استفاده می‌نمایند. Vmware ESXi دارای ویژگی های بسیار زیادی می‌باشد که ذکر آن‌ها در این مقاله نمی‌گنجد.

از آنجا که هایپروایزر ESXi تمرکز ویژه‌ای بر مسئله امنیت در محصولات خود دارد، ما قصد داریم تا برخی ویژگی های امنیتی ESXi را مورد بررسی و تحلیل قرار دهیم.

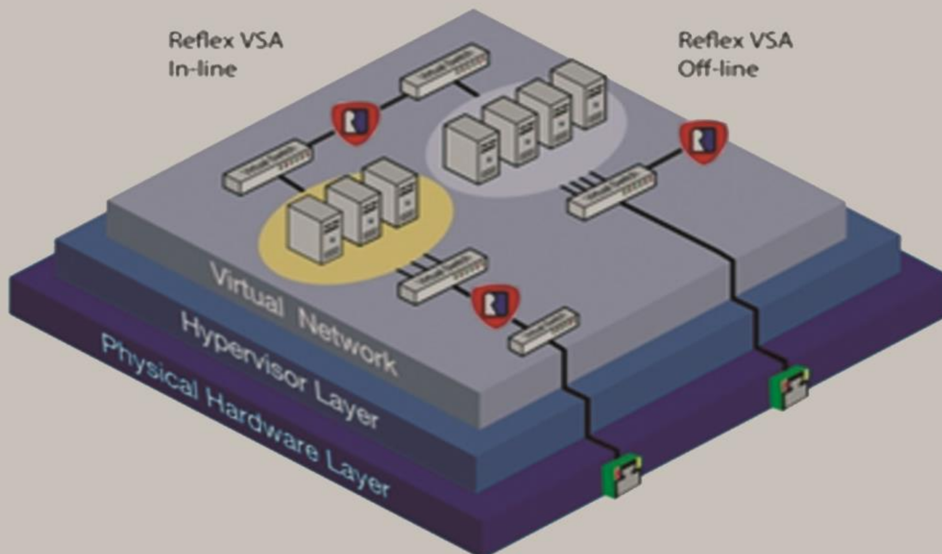


امنیت و لایه‌های شبکه مجازی

در مجازی سازی منظور از لایه شبکه همان کارت شبکه های مجازی و سوئیچ‌های مجازی هستند. هایپروایزر ESXi با تکیه بر لایه شبکه مجازی اتصال خود را با ماشین‌های مجازی میسر می‌سازد و از لایه شبکه برای اتصال به دستگاه‌های ذخیره‌ساز در انواع NAS , SAN استفاده می‌نماید. در Vmware به منظور امن سازی سیستم‌ها می‌توان از فایروال استفاده کرد که در Vmware توسط ابزارهای حرفه‌ای مجازی صورت می پذیرد. هم چنین ESXi از پروتکل IEEE ۸۰۲٫۱Q پشتیبانی می‌کند و همان طور که ذکر شد به شما امکان محافظت از شبکه‌های مجازی و شبکه‌های ذخیره سازی را به صورت پیشرفته میدهد. قابلیت تعریف Vlan نیز در ESXi پشتیبانی شده است و همان طور که می‌دانید Vlan به شما این امکان را می‌دهد که قسمتی از شبکه خود را از قسمت های دیگر جدا کرده و با این کار ضریب امنیت خود را افزایش دهید.

امنیت و ماشین‌های مجازی

در بستر Vmware ماشین‌های مجازی به صورت ایزوله فعالیت می‌کنند. اما ایزوله بودن سیستم عامل‌های ماشین مجازی به چه معناست؟ یعنی در صورت بروز مشکل در یک ماشین، دیگر ماشین‌ها می‌توانند بدون هیچ مشکلی و بدون اینکه اصلا متوجه مشکلی شوند، کار خود را بدون وقفه ادامه دهند.



محافظت ESXi از Vmkernel با ۳ قابلیت زیر:

: Memory Hardening

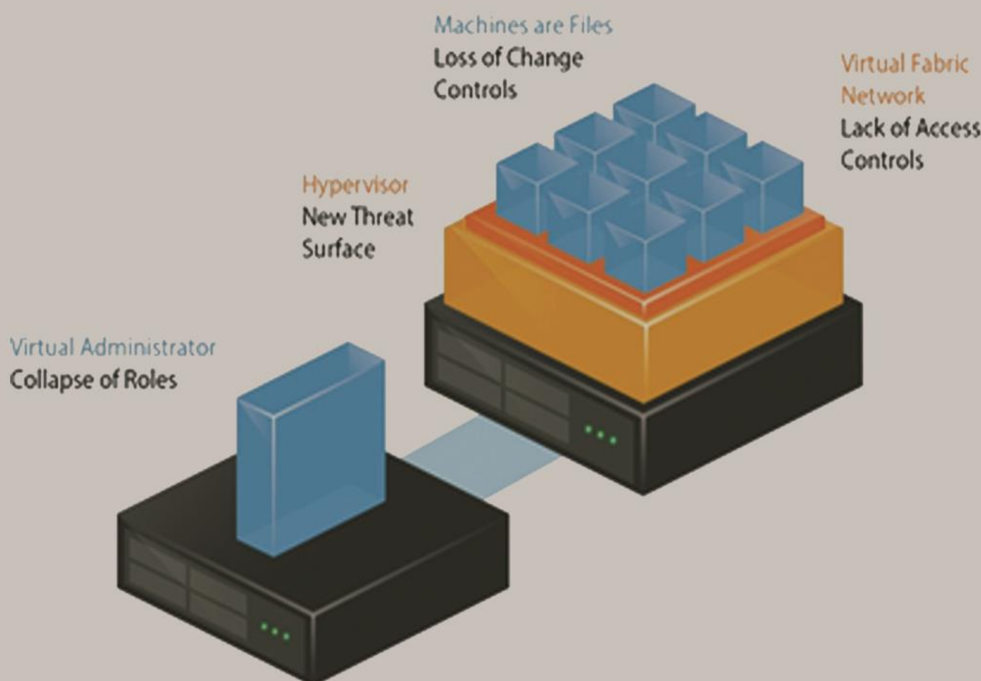
کرنل ESXi برنامه های کاربران و کامپوننت های اجرایی مانند کتابخانه‌ها را با استفاده از آدرس دهی تصادفی و غیز قابل پیش بینی حافظه، حفاظت می کند. این قابلیت vm ها را از آسیب پذیری Memory Ex-ploit محافظت می‌نماید.

: Kernel Module Integrity

امضای دیجیتال باعث اطمینان از صحت و احراز هویت ماژول¬ها، درایورها و برنامه‌ها که توسط VM-kernel بار می‌شوند می‌گردد. صحت عملکرد ماژول به ESXi این اجازه را می‌دهد که ماژول¬ها، درایورها، برنامه‌های کاربردی و certificate های VMware را شناسایی کند.

: Trusted Platform Module

TPM یک چیپ ست خاص است که بر روی بردهای کامپیوتر نصب شده است و به منظور احراز هویت فرد استفاده کننده از دستگاه مورد استفاده قرار می‌گیرد. در این نوع از احراز هویت TPM دستگاه از کاربر سؤال پرسیده و اطلاعات خاصی مانند کلید رمزنگاری، گواهینامه¬ های دیجیتال و مواردی از این دست را بر روی سیستم میزبان تعریف می‌نماید. وی ام‌ور از قابلیت‌های TPM به منظور حفظ امنیت پشتیبانی می‌کند



امنیت در هوش مصنوعی

تاریخچه ی هوش مصنوعی بسیار غنی است و به داستان ها و افسانه های مصر و یونان باستان باز می گردد. داستان هایی از ماشین ها و مخلوقاتی ساخته ی دست انسان که قدرت استدلال و تصمیم گیری داشته اند.



از افسانه ها که بگذریم ریاضی دانان و فیلسوفان از گذشته تا کنون مباحثی مربوط به استدلال و منطق را پیش کشیده اند که امروزه از این مباحث در هوش مصنوعی استفاده ی بسیاری می شود. این موضوع در سال ۱۹۵۰ با انتشار مقاله ای توسط الن تیورینگ بیش از پیش مورد توجه قرار گرفت و بعد از آن فراز و فرود هایی بسیاری داشته است . کاربرد های هوش مصنوعی آنقدر زیاد است که اگر فقط تصمیم به نام بردنشان داشته باشم می توانم چندین صفحه را به این امر اختصاص دهم.



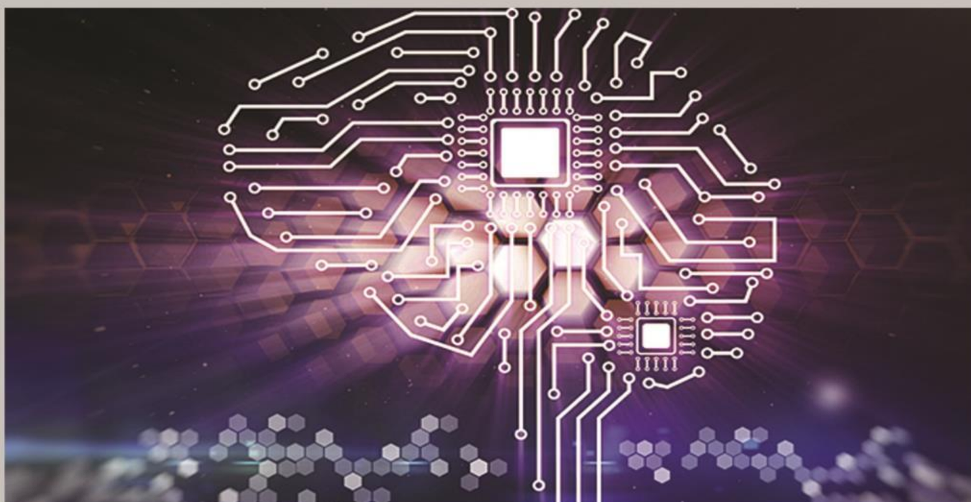
با توجه به اینکه هوش مصنوعی و حمله های سایبری ترکیب خطرناکی را به وجود می آورد دانستن کاربردهای هوش مصنوعی در دفاع سایبری و چشم اندازهایی از افزایش قابلیت‌های دفاع سایبری با استفاده از افزایش هوشمندی سیستم های دفاعی خالی از لطف نیست. تجربیات در رفع حملات DDos نشان می‌دهد که حتی یک مقاومت در برابر حملات با مقیاس بزرگ و کمترین منابع زمانی که روش‌های هوشمند استفاده می‌کنند، می‌تواند موفقیت آمیز باشد.

برای مثال، استفاده‌ی گسترده ازعلوم در تصمیم گیری‌ها بسیار ضروری بوده و پشتیبانی تصمیم گیری هوشمند هنوز یکی از مشکلات حل نشده در دفاع سایبری است. واضح است که دفاع در برابر سلاح های سایبری هوشمند تنها توسط نرم‌افزارهای هوشمند می‌تواند به دست آید و حوادث دو سال اخیر افزایش سریع هوشمندی نرم افزارهای مخرب و سلاح‌های سایبری را نشان می‌دهد. برای مثال میتوان به کرم Conficker اشاره کرد که برخی از تاثیر های این کرم روی شبکه های کامپیوتری پلیس و نظامی در اروپا به این شرح زیر است:

شبکه های کامپیوتری نظامی کشور فرانسه (Intra-mar)، در ژانویه سال ۲۰۰۹ به کرم Conficker آلوده شده بود. شبکه به حالت قرنطینه درآمده و هواپیماهای جنگنده‌ی چند فرودگاه به علت دانلود نشدن نقشه های پرواز به زمین نشانده شدند. وزارت دفاع انگلیس اعلام کرد که بخش عمده‌ای از سیستم‌های اصلی آنها و کامپیوترهای رومیزی‌شان آلوده به این ویروس شده. ویروس درتمام دفاتر اداری گسترش یافته بود، کامپیوتر های ناوهای جنگی سلطنتی، زیر دریایی‌های جنگی سلطنتی و بیمارستان‌های شهر شیفلد خبر از آلوده شدن حدود ۸۰۰ کامپیوتر می‌دادند.

یکی از شاخه های مهم هوش مصنوعی شبکه‌های عصبی است که در تشخیص نفوذ و ممانعت از نفوذ به خوبی قابل اجرا است. برای استفاده از آنها در تشخیص حمالات DDos، تشخیص کرم‌های کامپیوتری، تشخیص Spam، تشخیص Zombie، طبقه بندی بدافزارهای مخرب و تحقیقات قانونی پزشکی پیشنهادهایی وجود دارد. یکی از دلایل محبوب بودن شبکه های عصبی در دفاع سایبری، در سخت افزارها و پردازنده های گرافیکی باال بودن سرعت آنها است. پیشرفت های جدیدی در تکنولوژی شبکه های عصبی وجود دارد. شبکه های عصبیِ نسلِ سوم، شبکه های عصبی Spiking که از نورون های زیستی واقع بینانه تر تقلید می‌کنند، و فرصت های کاربردی بیشتری فراهم می‌کنند. فرصت‌های خوب توسط FPGA که توسعه سریع شبکه های عصبی و تنظیم آنها برای تغییرات نفوذی را قادر می‌سازد فراهم می‌شوند در حقیقت واضح نیست که چگونه توسعه سریع هوش مصنوعی ادامه می‌یابد، در هرصورت تهدیداتی وجود دارند که یک هوش‌مصنوعی سطح جدید ممکن است سریع تر از اینکه در دسترس باشد، از آن ها توسط عاملان حمله استفاده شود. ظاهرا، پیشرفت های جدید در فهم دانش، نمایش و بررسی در یادگیری ماشین می تواند به خوبی توانایی دفاع سایبری سیستم هایی که از آن ها استفاده می‌کنند باشد.

@Emitis



گیک و برنامه نویسی

در دنیای IT و تکنولوژی، برنامه نویسی نقش بسزایی در پیش برد اهداف یک شرکت و یا یک شخص دارد بطوری که اکثر شرکت ها برای ساخت و طراحی وب سایت و یا برنامه مخصوص آن شرکت برای Device های مختلف دست به دامان برنامه نویس ها شده اند. زبان های برنامه نویسی بسیار زیادی وجود دارد که هر شخص بسته به علاقه و نوع فعالیتی که قرار هست انجام دهد آنرا انتخاب می کند. امروزه دانستن هر نوع زبان برنامه نویسی نقطه قوتی برای شخص می باشد و می تواند به راحتی به کسب درآمد بپردازد. با توجه به رنکینگ جهانی مشخص شده است با داشتن دانش کدام یک از زبان های رایج برنامه نویسی می توانید درآمد بیشتری دریافت کنید .

Python

با توجه به بالا بودن تعداد زبان های برنامه نویسی تصمیم بر آن شد تا در مورد زبان برنامه نویسی Python اطلاعاتی را گرد هم آوریم و بررسی هایی را انجام دهیم. پایتون یک نوع زبان سطح بالا می باشد که حتی اگر کسی قبل از کار با این زبان هیچ آشنایی با زبان دیگری نداشته باشد می تواند آن را به سادگی فراگیرد.

در ۲۰ فوریه سال ۱۹۹۱ زبان برنامه نویسی پایتون توسط Guildo van Rossum طراحی و ارائه شد.





کم کم این زبان به یک زبان پرقدرت و سطح بالا تبدیل شد.

ویژگی هایی که پایتون را به یک برنامه سطح بالا تبدیل کرده interpreted, dynamic و readability بودن این زبان است.

Django and Flask

پایتون دارای فریم ورک های مختلف برای انجام کارهای متفاوت می باشد که می توان به Django و Flask اشاره کرد، این فریم ورک ها مختص به طراحی وب سایت می باشند و به وسیله این ها back-end یک سایت نوشته می شود. Django یک فریم ورک MVC یا به عبارتی Module View Control می باشد.

پایتون کتابخانه ای بزرگ دارد که می توان برای ساخت برنامه و نوشتن اسکریپت های مختلف به آن رجوع و از ماژول هایی که در اختیار کاربر قرار میدهد استفاده کرد .

به طور مثال می توان برای یک شبکه و سروری که مسئولیت های زیادی برای انجام کار دارد، به وسیله پایتون یک اسکریپت نوشت تا کارهای مربوطه را به موقع و بدون خطا اجرا کند. سایت های معروفی هم وجود دارد که از پایتون استفاده می کنند مانند سایت های فیس بوک، گوگل، یوتیوب، دراپ باکس، Quora و سایت Yahoo Map با فریم ورک Django طراحی شده اند.



با پایتون و رزبری در کنار هم می توان برنامه و طراحی های بسیاری را پیاده سازی کرد مانند : ساخت یک روتر در شبکه، فایروال، DNS Server و همچنین در زمینه رباتیک و هوش مصنوعی هم میتوان روی آنها حساب کرد.

برای مثال اگر بخواهیم تعدادی از پروژه هایی که به وسیله برد رزبری و زبان پایتون انجام شده را نام ببریم می توان به انتقال موزیک و چراغ های کریسمس سنسور سنجش رطوبت و دمای هوا،

ساخت سنسور اتوماتیک برای لوازم خانه و دستگاه بازی اشاره کرد.

@Bardimax



نفوذ ناپذیر

فایروال چیست؟

فایروال یا دیوار آتش به سخت افزار یا نرم افزارهایی گفته می‌شود که در Gateway شبکه قرار گرفته و داده های ورودی و خروجی را کنترل کرده و از دسترسی های غیر مجاز به کامپیوتر ها در یک شبکه یا اینترنت جلوگیری می کنند. فایروال یکی از مهم ترین لایه های امنیتی شبکه های کامپیوتری است که در صورت عدم وجود آن، خرابکارها و هکرها می توانند به راحتی و بدون هیچ محدودیتی وارد شبکه و سیستم‌ها شده و فعالیت های مورد نظر خود را انجام دهند.

فایروال همیشه در قسمت junction point شبکه، یعنی قسمتی که شبکه داخلی به شبکه های دیگر متصل می گردد یا با اینترنت ارتباط برقرار می کند، قرار می گیرد که به آن Edge شبکه نیز گفته می شود.

برای فایروال های سخت افزاری Rule هایی به صورت Default تعریف شده است که داده ها را فیلتر می کند. این Rule ها هرکدام دارای یک ویژگی خاص هستند و هرکدام از Rule ها از ورود و خروج داده های خاصی جلوگیری می کنند که البته می توان مطابق با Privacy سازمان مربوطه Rule های خاصی نوشته شود و اطلاعات مورد بررسی و آنالیز قرار گیرد.

فایروال همه داده ها را با Rule های خود مطابقت داده آن هایی که اجازه گذشتن از فایروال را دارند، Allow شده و مابقی Deny میگردند.



مسیر توسعه فایروال ها :

مسیر توسعه فایروال ها در غالب ۴ نسل جداگانه بررسی می گردند.

نسل اول : منظور همان فایروال های ساده هستند.

نسل دوم : قابلیت VPN (شبکه اختصاصی مجازی) به فایروال ها اضافه شد.

نسل سوم : همانند یک دروازه امنیتی عمل می کند و ویژگی های امنیتی زیر نسبت به نسل قبلی به آن اضافه شد:

– افزایش قابلیت VPN و ISP

– تشخیص هویت و مدیریت پهنای باند

– توسعه Rule Filtering

نسل چهارم : فایروال ها به UTM (سامانه مدیریت تهدید یکپارچه) مجهز شدند.



انواع فایروال ها :

در این نوع، فایروال هیچ کاری با محتوی بسته ارسالی یا دریافتی ندارد و فایروال ها با توجه به Header پکت های TCP/IP معیارهای خود را که در Rule ها Set شده اند با اطلاعاتی نظیر Source or Destination IP , Source or Destination PORT، زمان دریافت، TOS (نوع سرویس) و پارامترهایی این چنینی تصمیم به Allow or Deny کردن بسته ها می کند.

در این نوع فایروال ها چون با محتوی بسته کاری ندارند سرعت بالاتری نسبت به سایر فایروال ها دارد. این نوع فایروال ها در اکثر تجهیزات شبکه ای همچون روتر و سوئیچ وجود دارند.

Software Firewall

فایروال های نرم افزاری در قالب برنامه های قابل نصب برای سیستم عامل های مختلف هستند و بهترین انتخاب برای سیستم های خانگی.البته ذکر این نکته نیز قابل ذکر است که این نوع فایروال ها فیلترینگ های خاصی ندارند و بیشتر برنامه ها را فیلتر می کند و در اکثر آن ها برای نصب برنامه مجبور به خاموش کردن آن ها هستیم و در خیلی از سیستم های خانگی آنتی ویروس ها کنترل فایروال را بدست می گیرند.



Hardware Firewall

این نوع فایروال ها فایروال های شبکه هستند. بین دامین و شبکه داخلی اینترنت قرار می گیرند و در مواردی که سازمان ها قصد محافظت از رایانه های داخلی سازمان را دارند . از این نوع فایروال ها بهره میبرند. این نوع فایروال ها دارای سیستم عامل های مخصوص خود هستند که هسته اکثرآن ها یونیکسی میباشد و استفاده از آن ها باعث ایجاد یک لایه دفاعی در مقابل تهاجمات است.



Application Firewall

این نوع فایروال ها کل یک بسته را آنالیز می کنند یعنی هم header بسته ها و هم محتوی داخلی آن ها را بررسی می کنند و فیلتر اصلی روی محتوی آن ها صورت می گیرد.این نوع فایروال ها در تمامی مراحل هفت گانه مدلینگ OSI کار میکنند.

لایه یک تا چهارم که عمل مسیر یابی و لایه های پنجم تا هفتم که مربوط به انتقال داده ها هستند. بخش اصلی پکت ها همان محتوی آن هاست.این نوع فایروال ها قابلیت ایجاد rule filtering هایی دارند که محتوی بسته ها را بررسی میکند. چون بررسی و آنالیز محتوی بسته ها بسیار زمان بر است بنابراین سرعت این نوع فایر وال ها نیز کندتر است.

Proxies Firewall



سرور های پراکسی نوعی رابط میان یک شبکه و یک شبکه دیگر با یک کاربر و اینترنت است که برای مواردی همچون حفظ امنیت، پنهان کردن هویت و ... کاربرد دارد. در این نوع سرور ها کاربر مستقیما درخواست خود را به مقصد مورد نظرش ارسال نکرده و مستقیما جوابی دریافت نمی کند بلکه در خواست خود را به سرور پراکسی فرستاده و پراکسی در صورت نیاز به پردازش هایی روی آن انجام داده و از آنجا برای مقصد ارسال می کند.

فایروال پراکسی نوعی فایروال است که بر روی سرور پراکسی قرار می گیرد و کاربر با وصل شدن به آن در واقع به یک فایروال وصل شده است. در این حالت داده ها در طول مسیر فیلتر می شنوند و محتوی آن ها بررسی می گردد.

اما این فایروال ها مشکلاتی را نیز دارند.اطلاعات ممکن است در سرور پراکسی دزدیده شود و یا کنترل کامل اطلاعات بدست پراکسی بیافتد.

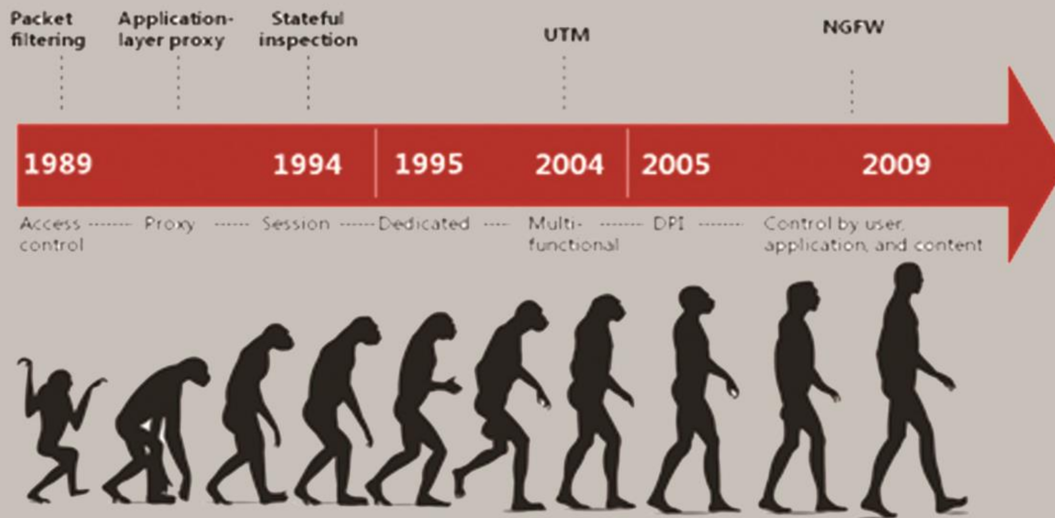
ویژگی ها و فایروال های امروزی:

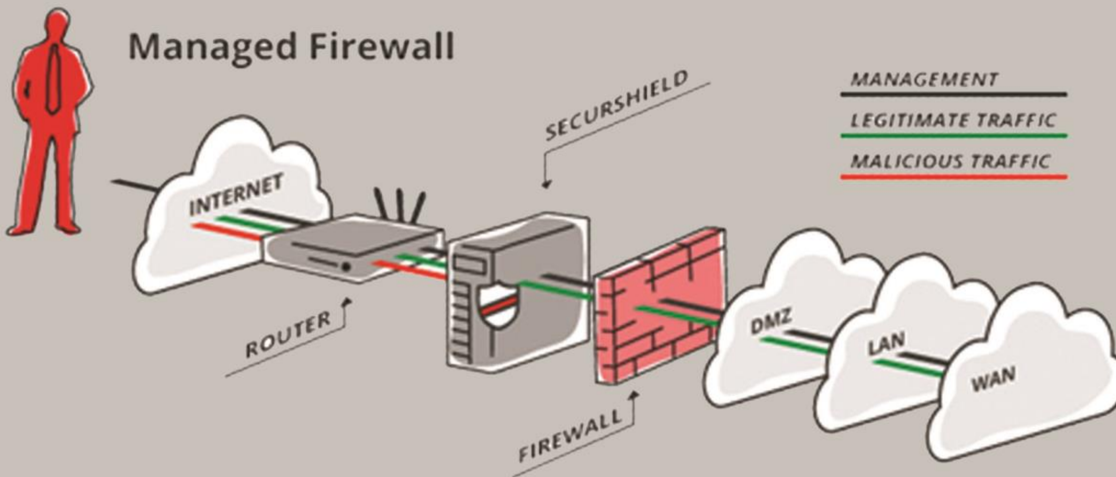
این فایروال ها برای ارائه مکانیزم های مختلف امنیتی در شبکه های کوچک تا خیلی بزرگ هستند.

این محصولات ترافیک . Vpn , تشخیص و جلوگیری از تشخیص هویت ترافیک تصفیه محتوی وب و مدیریت پهنای باند را ارائه میدهند.

با استفاده از مکانیزم تشخیص هویت ترافیک امکان تعریف سیاست های امنیتی سازمان را مبتنی بر کاربران و گروه های کاربری فراهم می کند.

همچنین با استفاده از قابلیت های failover قابلیت اطمینان بسیار بالایی را در صورت قطع برق و خرابی سخت افزار تامین می نماید.





برخی ویژگی های دیگر :

کنترل محتوی در سطح لایه کاربرد

مدیریت متمرکز و یکپارچه

ارائه سرویس های امنیتی پیچیده

کاهش پیچیدگی

سادگی نصب

حداقل نیاز برای تعامل با اپراتور

عیب یابی آسان

@Geek_072



sketch
IDEA
PHP
</>
HTML5
.com
JAVA
CSS3